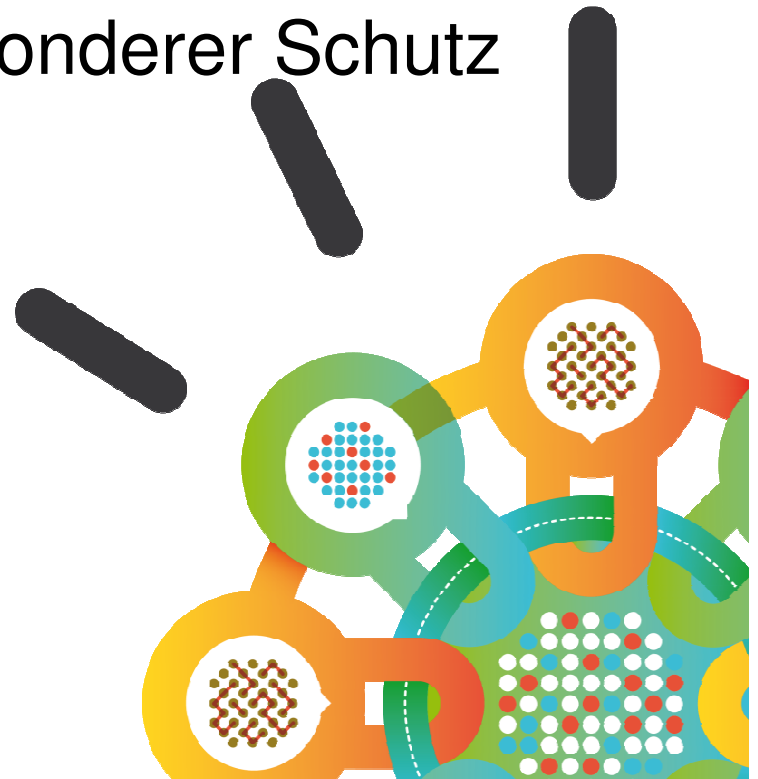


Security Intelligence.
Think Integrated.

Security für den Mainframe

Besondere Informationen, besonderer Schutz

Martina Schmidt
Senior Technical Sales Professional
martina.schmidt@de.ibm.com



Mainframe Security for Dummies® (in 2 Seiten)

1. Laut Gartner ist der IBM z/OS Mainframe weiterhin ein sehr wichtige Plattform für viel Unternehmen, auf denen ca. 90% der geschäftskritischen Anwendungen betrieben werden.
 - Bis zu 65% aller weltweiten Daten liegen auf Mainframes
2. Mainframe Spezialisten sind gefragt
3. RACF (Resource Access Control Facility) ist das Identity und Access Management Tool für den Mainframe und wird auf 80% aller Mainframes eingesetzt, andere Produkte sind ACF2 und TopSecret
 - Die Administration von RACF erfordert spezielles Know-How
 - zSecure bietet eine benutzerfreundliche Administrationsoberfläche für RACF



® Registered Trademark of Dummies.com

Mainframe Security for Dummies® (in 2 Seiten)

4. RACF bietet kein Compliance Monitoring, Reporting oder Überwachung hochberechtigter Benutzer
 - zSecure bietet diese Möglichkeiten sowohl für RACF, als auch für ACF2 und TopSecret
5. Einige Unternehmen haben eigene Skripte entwickelt, um Complianceanforderungen gerecht zu werden
 - Solche Skripte wurden größtenteils bereits vor Jahren geschrieben und sind meist nicht ausreichend dokumentiert
 - zSecure beseitigt diese Sorgen



® Registered Trademark of Dummies.com



Zum Vergleich:

Enter TSO or Workstation commands below:

===> lu

```

USER=SCHMIDT  NAME=TINA SCHMIDT          OWN
DEFAULT-GROUP=SYSMGT  PASSDATE=10.271 PASS
ATTRIBUTES=SPECIAL OPERATIONS
ATTRIBUTES=AUDITOR
REVOKE DATE=NONE  RESUME DATE=NONE
LAST-ACCESS=12.055/16:12:18
CLASS AUTHORIZATIONS=NONE
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED    (DAYS)          (TIME)
*** _

```

```

ANYDAY
GROUP=SYSMGT  AUTH=USE  CONNECT-OWNER=SYSMGT  CONNECT-DATE=07.192
CONNECTS=    918  UACC=NONE  LAST-CONNECT=12.055/16:12:18
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=USERS    AUTH=USE  CONNECT-OWNER=USERS    CONNECT-DATE=07.192
CONNECTS=     00  UACC=NONE  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=DATAMGT  AUTH=USE  CONNECT-OWNER=DATAMGT  CONNECT-DATE=07.192
CONNECTS=     00  UACC=NONE  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=C2RSERVG AUTH=USE  CONNECT-OWNER=C2RSERVG  CONNECT-DATE=10.075
CONNECTS=     00  UACC=READ  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=C2RGROUP AUTH=USE  CONNECT-OWNER=C2RGROUP  CONNECT-DATE=10.075
CONNECTS=     00  UACC=READ  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=SWMGTT   AUTH=USE  CONNECT-OWNER=CAHINZ  CONNECT-DATE=10.271
CONNECTS=     00  UACC=NONE  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=SYSAUDIT AUTH=USE  CONNECT-OWNER=CAHINZ  CONNECT-DATE=10.271
CONNECTS=     00  UACC=NONE  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE  RESUME DATE=NONE
GROUP=ZSECWS   AUTH=USE  CONNECT-OWNER=SCHMIDT  CONNECT-DATE=10.301

```

Zum Vergleich:

Identification of SCHMIDT

User name

Installation data

Owner

User's default group

Group	Auth	R	SOA
JAVAWS	USE	-	SOA
C2RGROUP	USE	-	-
C2RSERVG	USE	-	-
DATAMGT	USE	-	-
SWMGT	USE	-	-
SYSAUDIT	USE	-	-
SYSMGT	USE	-	-
USERS	USE	-	-
ZSECWS	USE	-	-

System access

Revoked (may be by date)

Inactive, revoked or pe

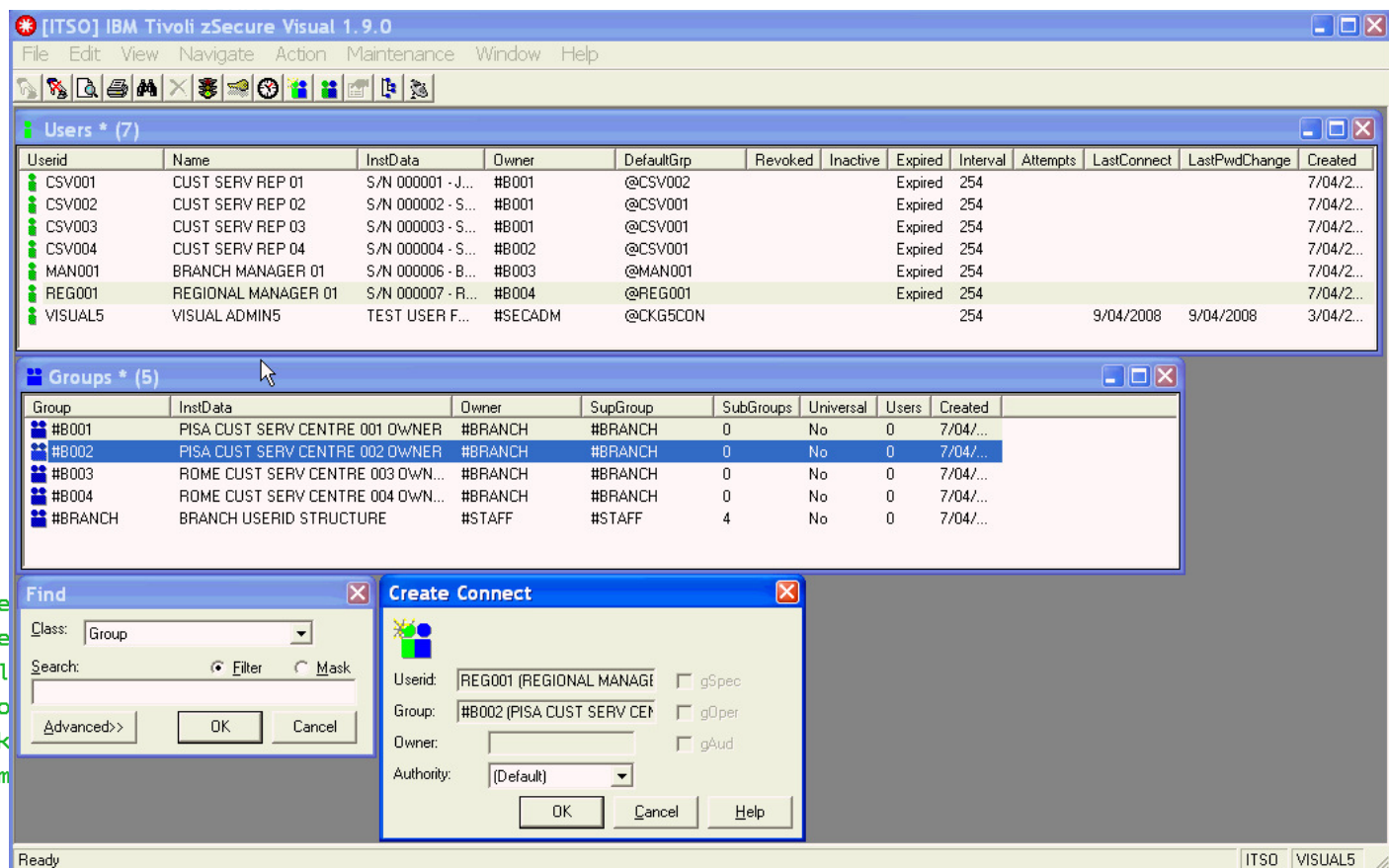
Days of week user can l

Time of day user can lo

Date user will be revok

Date user will be resum

SYS1



[ITSO] IBM Tivoli zSecure Visual 1.9.0

File Edit View Navigate Action Maintenance Window Help

Users * (7)

Userid	Name	InstData	Owner	DefaultGrp	Revoked	Inactive	Expired	Interval	Attempts	LastConnect	LastPwdChange	Created
CSV001	CUST SERV REP 01	S/N 000001 - J...	#B001	@CSV002			Expired	254				7/04/2...
CSV002	CUST SERV REP 02	S/N 000002 - S...	#B001	@CSV001			Expired	254				7/04/2...
CSV003	CUST SERV REP 03	S/N 000003 - S...	#B001	@CSV001			Expired	254				7/04/2...
CSV004	CUST SERV REP 04	S/N 000004 - S...	#B002	@CSV001			Expired	254				7/04/2...
MAN001	BRANCH MANAGER 01	S/N 000006 - B...	#B003	@MAN001			Expired	254				7/04/2...
REG001	REGIONAL MANAGER 01	S/N 000007 - R...	#B004	@REG001			Expired	254				7/04/2...
VISUAL5	VISUAL ADMIN5	TEST USER F...	#SECADM	@CKG5CON				254		9/04/2008	9/04/2008	3/04/2...

Groups * (5)

Group	InstData	Owner	SupGroup	SubGroups	Universal	Users	Created
#B001	PISA CUST SERV CENTRE 001 OWNER	#BRANCH	#BRANCH	0	No	0	7/04/...
#B002	PISA CUST SERV CENTRE 002 OWNER	#BRANCH	#BRANCH	0	No	0	7/04/...
#B003	ROME CUST SERV CENTRE 003 OWN...	#BRANCH	#BRANCH	0	No	0	7/04/...
#B004	ROME CUST SERV CENTRE 004 OWN...	#BRANCH	#BRANCH	0	No	0	7/04/...
#BRANCH	BRANCH USERID STRUCTURE	#STAFF	#STAFF	4	No	0	7/04/...

Find

Class: Group

Search: Filter Mask

Advanced> OK Cancel

Create Connect

Userid: REG001 (REGIONAL MANAGI ☐ gSpec

Group: #B002 (PISA CUST SERV CET ☐ gDper

Owner: ☐ gAud

Authority: (Default)

OK Cancel Help

Ready

ITSO VISUAL5

Herausforderungen um Mainframe Security

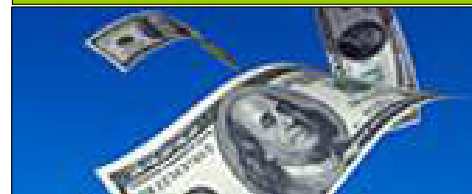
Compliance



Steigende Komplexität



Steigende Kosten



▪ **Compliance:**

- Compliance Nachweis oft manuelle Aufgabe
- Alarmierungen erfolgen zu spät (wenn überhaupt)

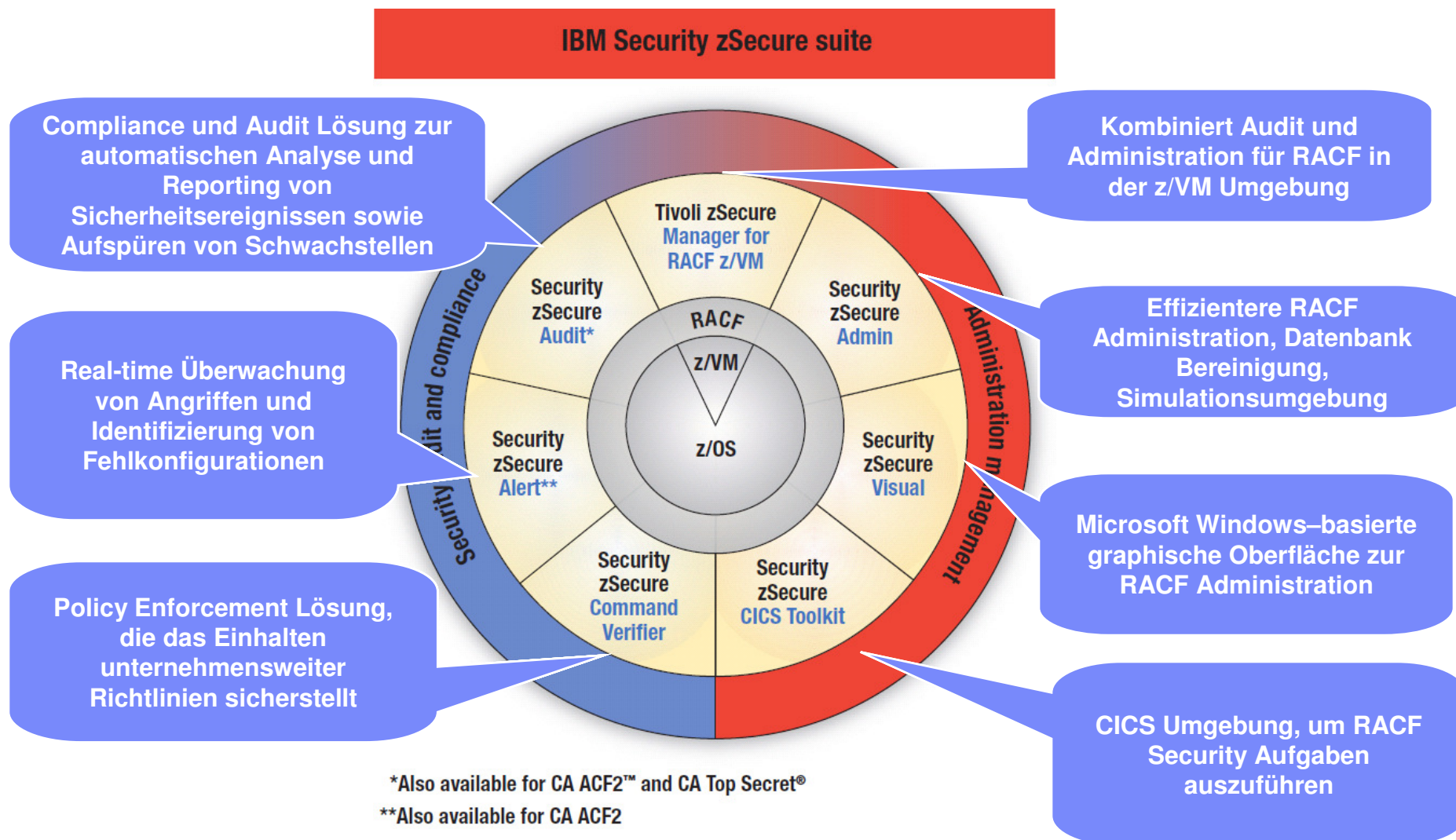
▪ **Komplexität:**

- Mainframe ist integraler Bestandteil der meisten komplexen Geschäftsanwendungen, was die Identifizierung und Analyse von Sicherheitsrisiken schwierig macht
- Aktionen hochberechtigter Benutzer, die nicht in Genehmigungsprozesse eingebunden sind

▪ **Kosten:**

- Mainframe Security Administration erfolgt meist manuell oder über wenig dokumentierte Skripte
- Administration wird von gut ausgebildeten Mainframe Spezialisten durchgeführt, die am Markt sehr gefragt sind

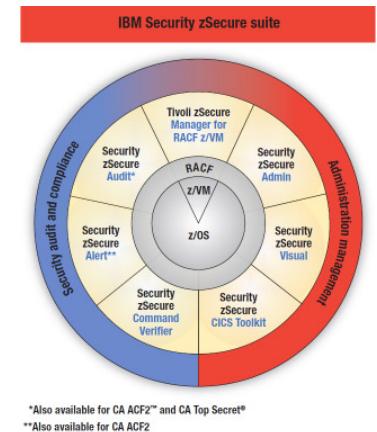
IBM Security zSecure Suite Überblick



Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

[Referenz] Geschäftsvorteile der zSecure Suite

- Reduzierung von Kosten durch effizientere Administration
 - Automatisierung von Administrationsaufgaben
 - Benutzerfreundliche Schnittstelle
 - Verbesserte Systemverfügbarkeit durch automatische Analyse und Ermittlung von Schwachstellen und Konfigurationsänderungen
- Proaktives Compliance Monitoring
 - Automatisiertes Compliance Monitoring, auf den Kunden angepasst, real-time Alarmierungen bei Bedrohungen, unerlaubten Datenzugriff oder Fehlkonfigurationen
 - Abwehren von gefährlichen RACF Kommandos, um Missbrauch durch hochberechtigte Benutzer zu verhindern
 - Automatisierte Datensammlung für Compliance Reporting, Audit Trail Analyse
- Effizienz- und Qualitätssteigerung
 - Automatische Funktionen reduzieren Fehler, die zu Datenverlust und kostspieligen Ausfällen führen können
 - Single point of Administration für große und kleine z/OS Umgebungen und mehreren RACF Datenbanken
 - Optimierte Verwaltung von hochberechtigten Benutzern zur Identifizierung und Entfernung unnötiger Berechtigungen



Wie können wir helfen?

From zero to zHero – Workshop Woche

- 08.-10.05.2012, IBM Frankfurt
- Vortrag & Demo: **RACF Database Cleanup**
- <http://www-05.ibm.com/de/events/fromzerotozhero/index.html>

Sicherheit im Zentrum

- Individuell, inhouse
- <http://www-05.ibm.com/de/events/securityworkshop/index.html>

- Ansprechpartner für Vorträge, Demonstrationen, PoC's:



Carsten Hinz [more info](#)

carsten.hinz@de.ibm.com

49-172 654 99 76 M: 49-172-654 99 76

Hamburg, DE IBM Sales & Distribution, Software Sales

Leading Technical Sales Professional - Certified IT Specialist



Martina Schmidt [more info](#)

martina.schmidt@de.ibm.com

49-175 7280739 M: 49-175 7280739

Ehningen, DE IBM Sales & Distribution, Software Sales

Senior Technical Sales Professional / Pan-IMT Security on System z / zChampion